



**STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE**

Policy No. DOC 1.7.9	Subject: ACCEPTABLE USE OF IT RESOURCES
Chapter 1: ADMINISTRATION AND MANAGEMENT	Page 1 of 4
Section 7: Information Systems	Effective Date: Dec. 1, 1996
Signature: /s/ Mike Batista, Director	Revised: 07/23/14

I. POLICY

The Department of Corrections maintains exclusive ownership and control of Information Technology (IT) resources used for Department business, provides guidelines on acceptable and prohibited use of IT resources, and permits limited personal use of IT resources by Department employees as defined in this policy.

II. APPLICABILITY

All divisions, facilities, and programs Department-owned or contracted, as specified in the contract.

III. DEFINITIONS

Download – To copy software programs, games, screen savers and other such items from the Internet to a Department IT resource. Download does not include the copying of text documents from the Internet to a Department IT resource.

Department Employee – The term includes paid employees or contracted persons (temporary or permanent), volunteers and interns who are paid or donate time or services to the Department, contractors, on-site vendors and individual service providers, e.g. delivery, maintenance, vendors, etc. who may not be contracted to the Department and whose assignment is primarily on Department premises, e.g. facility or program offices.

External Media Device – USB drives, digital cameras, multimedia players, smartphones and tablets, DVD's or CD's.

Information Technology (IT) Resources – Any computer system, including but not limited to, computers, servers, printers, smartphones, tablets, laptops, and networks.

Internet – An electronic communications network that connects computer networks and organizational computer facilities around the world.

Public Record – Any paper, correspondence, form, book, photograph, microfilm, magnetic tape, computer storage media, map, drawing or other document, including all copies thereof, regardless of physical form or characteristics, that have been created or received by a state agency or local government in connection with the transaction of official business. It includes all records or documents required by law to be filed with or kept by the Department.

SummitNet – The State of Montana's telecommunications nucleus network or backbone connecting agency, university, grades K-12, library, and local government networks. SummitNet provides connectivity to the Internet.

Policy No. DOC 1.7.9	Chapter 1: Administration and Management	Page 2 of 4
Subject: ACCEPTABLE USE OF IT RESOURCES		

IV. DEPARTMENT DIRECTIVES

A. Use of IT Resources

1. Department supervisors and managers are responsible for ensuring Department employees follow the provisions of this policy in the use of Department IT resources in accordance to [DOC 1.7.6 Unlawful Use of IT Resources](#).
2. Employees do not have a right of privacy in their use of IT resources. Agency system administrators, management, and Department of Administration personnel may monitor all aspects of employee usage of IT resources.
3. Department employees may only use IT resources to conduct state business, except as otherwise noted in this policy. Employees are responsible for the appropriate use and safe-keeping of IT resources. Supervisors may prohibit or limit employee use of IT resources at any time for business-related reasons.
4. IT resources may not be used for the employee's private for-profit or not-for-profit business activities as identified in [2-2-121\(2\), MCA](#) or for fraternal or association activities not related to the employee's position and job duties.
5. Employees must comply with all applicable local, state, and federal laws, telecommunications and network regulations, or policies including, but not limited to: copyright laws, commercial software and intellectual property laws and regulations; i.e. downloading a copyright protected cartoon or graphic for use in a publication without an appropriate copyright release.

B. Acceptable Use of Distribution Lists

1. To efficiently distribute Department-wide communications such as policy notifications, legislative information, budget updates, and other core business activities, the Department has established an e-mail distribution list titled *Cor Policy Distribution*. Employees should limit use of this distribution list to only the aforementioned subjects.

C. Acceptable Personal Use of IT Resources

1. Acceptable personal use includes e-mail for essential personal communication such as messages to family members, significant others, teachers, doctors and day-care providers to communicate work schedule changes, status, or other personal business. Acceptable Internet use includes personal information gathering during lunch breaks and non-working hours, as long as it does not interfere with staff productivity or preempt any business activities. Violation of this section may lead to employee discipline, up to and including termination.

D. Prohibited Personal Use of IT Resources

1. The following activities are prohibited unless directly related to job duties such as Department criminal conduct investigations, or in connection with personnel actions.
 - a. Transmitting, retrieving or storage of any materials:

Policy No. DOC 1.7.9	Chapter 1: Administration and Management	Page 3 of 4
Subject: ACCEPTABLE USE OF IT RESOURCES		

- 1) defined as obscene by [45-8-201\(2\) MCA](#);
- 2) advocating or portraying sexual conduct involving children as identified in [45-5-625 MCA](#);
- 3) advocating violence against others or their property, because of race, creed, religion color, national origin, disability or involvement in civil rights or human rights activities as provided in [45-5-221 MCA](#);
- 4) advocating violence against others or their property because of sexual orientation;
- 5) promoting political candidates or personal political issues; and
- 6) generating or circulating chain letters.

E. E-Mail

1. Staff communications via state e-mail are usually public documents and may be maintained for future retrieval.
 - a. Employees may delete the following e-mail messages because they are not considered public documents:
 - 1) notices without official business value;
 - 2) junk mail such as spam, vendor solicitations, promotional materials, reference files copied or downloaded from Internet sites, or other unsolicited non-record messages;
 - 3) secondary copies generated by another agency or user who, as the originator, has the responsibility for keeping the official “record copy;” and
 - 4) publications generated by another entity or user, who as the originator has the responsibility for keeping the official “record copy.”
2. If an e-mail item needs to be retained, it should be moved to an off-line personal folder, archive folder, or be printed.
3. [DOC Policy 1.2.7, Inventories/Records Management](#), should be referred to for additional questions about retention of e-mail public records.

H. Downloading or Installing Software/Hardware

1. Employees may not use or install any software or hardware on a state IT resource unless approved and procured by the Department; this includes USB drives, CDs, DVDs, iPods, other portable media players, personal digital assistants (PDAs), cell phones, and digital cameras.
2. Employees may not download or install software not specifically licensed to the Department and approved by the NSB Chief through the Information Technology Purchase Request (ITPR) process including all shareware, freeware and Beta release software products.

I. Department-Owned Portable IT Resources

1. Employees who use a Department-owned portable IT resource must:
 - a. lock a vehicle if the IT resource is inside of it;
 - b. let the IT resource warm to room temperature before starting it up after removing it from a vehicle during cold weather;

Policy No. DOC 1.7.9	Chapter 1: Administration and Management	Page 4 of 4
Subject: ACCEPTABLE USE OF IT RESOURCES		

- c. not allow unsupervised use of an IT resource while at home;
- d. protect the IT resource from unauthorized use through safeguards to include, but not limited to, a password, pattern gesture, smart card or biometric, etc.; and
- e. follow Department policy, procedure, and guidelines regarding the use of IT resources.

K. Reporting and Disciplinary Action

1. Users will:
 - a. cooperate with the requests of the NSB chief, or designee, for information about computing activities;
 - b. follow agency procedures and guidelines in handling external media in order to maintain a secure, virus-free computing environment; and
 - c. follow agency procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location.
2. Users will report unacceptable use and security violations to their immediate supervisors or appropriate IT staff responsible for the security and enforcement of network policies where the violation originated.
3. If there is reasonable cause to suspect an employee has violated this policy, immediate suspension of access to IT resources pending further investigation may result. Confirmed violations will subject employees to disciplinary action up to and including termination under [3-0130, Disciplinary Action, Montana Operations Manual \(MOM\)](#).

V. CLOSING

Questions concerning this policy should be directed to the Department's Chief Information Officer (CIO).

VI. REFERENCES

- A. [2-2-121](#), MCA; [2-6-101](#), MCA; [2-6-202](#), MCA; [2-15-112](#), MCA; [2-15-114](#), MCA; [2-17-504](#) through [528](#), MCA; [2-17-533](#), MCA; [18-4-313](#), MCA; [45-5-221](#), MCA; [45-5-625](#), MCA; [45-6-311](#), MCA; [45-8-201](#), MCA; [45-8-213](#), MCA; [53-1-203](#), MCA
- B. *Article II, Section 9; Montana Constitution*
- C. *Volume 1, Chapters 1-0200.00 through 1-0250.30; Chapters 1-1100.00 through 1-1110.00; Vol. III, Chapter 0130; Montana Operations Manual (MOM)*
- D. *2-12-1 & 2; 2-13-101-107; Administrative Rules of Montana*
- E. *DOC Policies [1.2.7](#), Inventories/Records Management; [1.3.2](#), Employee Performance and Conduct Guidelines*

VII. ATTACHMENTS

None.